KTH Computer Science
and Communication

Proof of Work

An evaluation of proof of work as a DOS prevention method

FREDRIK LILKAER, CHRISTOPHER TELJSTEDT

Bachelor's Thesis
Supervisor: Douglas Wikström

1 Introduction

Denial of Service continues to plague internet services, as evidenced by the recent attack on Spamhaus [1]

It is essentially a targeted effort to prevent a service from functioning properly by draining the underlying computer resources. Such an attack is executed by having each attacking machine performing only small load of total work, relying on the cumulative work to overload target system.

This paper focuses on Proof of Work, a concept originally proposed by Dwork and Naor in their report "On Memory-Bound Functions for Fighting Spam", as an approach to fighting denial of service attacks. The "proof of work" is cryptographic in flavor and the idea is essentially to respond with a problem that is moderately hard to compute but easy to verify. Dwork and Naor originally called this a *pricing function* because of it's economic origin. They introduced this concept as a way to fight e-mail spam by increasing the costs of sending spam, thus making e-mail spam economically unfeasible.

1.1 Background

One of the most significant threats in server security are Denial of Service (DoS) attacks. It is essentially a targeted effort to prevent a service from functioning properly by draining the underlying computer resources. There are different levels of the attacks which either can be targeted to exploit vulnerabilities in the TCP/IP-protocol, in the operation system that the server runs on or more specific implementations of the service. [källa på det här]

1.2 Problem definition

Proof of Work has been shown to potentially work as a prevention mechanism to at least mitigate the effects of a DoS attack without making an as assumption about the source.[källa] However, Laurie and Clayton concluded in the paper *Proof-of-Work" proves not to work*, that PoW on it's own, is not a feasible solution to fighting spam and denial of service attacks. This is because the classical implementation of Proof of Work does not seperate legitimate users from attackers. Hence, problems from a Proof of Work protected system would not discourage abusers of the system without having an unacceptable effect on legitimate users.

This was not that was unthought of when Proof of Work was first proposed.

1.3 Problem statement

With the problem defined the question at hand is thus if it is possible to develop a Proof of Work protocol that is independent of client characteristics.

- Is there a viable way to implement a Proof of Work system so that the system's resources are accessable by a diverse variety of devices?

- How should the protocol be optimised for low impact on legitimate client behaviour and high impact on malicious behaviour?

- What advantages and disadvantages does proof of work concept bring in practice and in which applications could it be an improvement to current security?

2 Purpose and method

The purpose of this study is to research ways to improve the classical Proof of Work in such a way that legitimate users are less affected by the Proof of Work than the participants of a DoS attack. Furthermore find a way to dynamically scale the required proof of work when dealing with different hardware.

2.1 Scope and delimitations

Scope:
The coverage of this study .....
The study consists of .....
The study covers the .....
This study is focus on .....

Delimitations:
The study does not cover the .....
The researcher limited this research to .....
This study is limited to .....

Bibliography

[1] BBC News Dave Lee Technology reporter. *Global internet slows after 'biggest attack in history'*. 2013. URL: `http://www.bbc.co.uk/news/technology-21954636` (visited on 04/06/2013).

[2] Cynthia Dwork, Andrew Goldberg, and Moni Naor. "On Memory-Bound Functions for Fighting Spam". In: *In Crypto*. Springer-Verlag, 2002, pp. 426–444.

[3] Ben Laurie and Richard Clayton. *Proof-of-Work" proves not to work*. 2004.